Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**497**
Land:	Myanmar
Kilde:	Article 19 m.fl.
Titel:	Resist Myanmar's digital coup: International community must dismantle military dictatorship – or reap repercussions
Udgivet:	Februar 2023
Optaget på baggrundsmaterialet:	20. juni 2023

Resist Myanmar's digital coup: International community must dismantle military dictatorship – or reap repercussions

Today marks two years since the Myanmar military initiated a deadly coup, ripping the country out of democratic transition. More than 700 days since the start of the coup and this bloody invasion now extends to the digital sphere where the military's tightening stranglehold translates to brutal rights violations against the people.

Ahead of the so-called elections later this year, the military continues to build and implement a complex attack and surveillance infrastructure with the help of private businesses.

Myanmar's telecommunications sector is now entirely controlled by the military – setting the stage for unprecedented surveillance. When the last two internationally-owned telecom operators in Myanmar, Telenor and Ooredoo, sold their operations in the country, the military gained the power to activate intercept surveillance across networks — a way to track, target, and eliminate those who resist the regime. It also now has access to a propaganda infrastructure that can spread the military's violent calls as often as possible. It was recently reported that prior to the coup, Israeli company, Cognyte Software Ltd, won a tender to sell intercept spyware to a state-backed telecommunications firm in Myanmar.

The military continues to shut down the internet to hide brutal human rights violations. Internet, wifi, mobile and landline connections are regularly shut down, most often in regions where resistance against the military is strongest. Communications blackouts are often imposed to shroud killings, ill-treatment, village burning, and other serious abuses. In 2022, all townships in Myanmar have experienced internet shutdowns.

When people are online, they are subjected to constant surveillance, doxxing, rampant discriminatory hatred, and violent incitement. The military and military-linked actors dart from one platform to another, spreading hateful and violent propaganda to provoke real world harms. Actors inciting hate primarily use Facebook, YouTube, TikTok, and Telegram, and easily reestablish accounts and online followings if and when companies finally remove their content. There have been numerous arrests of people who have used social media posts to support the resistance movement. Doxxing on Telegram is continuing unabated, as personal information and sexual content is shared on channels with thousands of followers, facilitating vigilante violence, mass shaming, and harassment, especially against women. Telegram must invest in addressing these harms and engage with civil society to put in place rights-based safeguards.

People are forced to surrender personal data that the military can use to facilitate more harm. SIM card and IMEI registrations are now required, and those who refuse to comply are immediately cut off from internet and mobile services. From these registrations, the military can gather residence addresses and location data or set the stage for false accusations of financing terrorism leading to deactivating mobile payment accounts.

Surveillance online and on the streets is a daily reality in Myanmar, and freedom of movement is severely restricted. Closed circuit television (CCTV) systems with facial recognition technology are now in at least ten cities and the infrastructure continues to expand in other parts of the country. These CCTVs are being sold by Zhejiang Dahua Technology, Huawei Technologies Co Ltd, and Hikvision — businesses that have been sanctioned for their products' use in Xinjiang, China, where surveillance has allegedly facilitated crimes against humanity. Reports are also emerging that military officers are conducting random house visits in villages and phone checks on the streets. Passport issuance has also stopped since December 2022, preventing people from leaving the country.

As long as the military remains desperate to gain international legitimacy, there is leverage to resist this coup, both online and offline. Continued inaction costs lives.

The international community must:

- Publicly condemn and push back against assaults on rights by the military and supportive private actors;
- Support calls for governments to scrutinize the sale of products to the Myanmar military to make sure these are not being used to facilitate human rights violations, and take further steps to enforce and tighten measures aimed at restricting the sale and supply of dual-use surveillance technologies to Myanmar;
- Hold companies accountable for apparent failures to respect human rights through their operations in Myanmar; and
- Provide support in various forms to the people of Myanmar, including human rights defenders, civil society, and journalists who face immense risk for their work.

Companies must:

- Use heightened due diligence to ensure that their products and services are not being used by the military and military-controlled institutions in violation of human rights, including

immediately removing these from the market when these are being used to facilitate rights abuses.

- Invest significant resources to implement human rights-based content moderation, data protection, and privacy safeguards to resist increasing attempts to extend surveillance, censorship, and abuse of rights;
- Pursue genuine public engagement in its decision-making process and implement effective remedies when human rights violations are committed.

Signatories:

Access Now

ACDD

Article 19

Athan - Freedom of Expression Activist Organization

CIVICUS: World Alliance for Citizen Participation

Digital Resilience Asia (DRA)

Digital Rights Collective

EngageMedia

Enlightened Myanmar Research Foundation (*EMReF)*

Free Expression Myanmar

Foundation for Media Alternatives

Heartland Initiative

Nar Sin Thu Myar

Nyan Lynn Thit Analytica

Open Observatory of Network Interference (OONI)

Reporters without Borders

SAFENet-Southeast Asia Freedom of Expression Network

Sisters2Sisters

Spring Sprouts

Thai Netizen Network